MUHA LAJOS

AZ INFORMATIKAI BIZTONSÁG EGY LEHETSÉGES RENDSZERTANA[1]

Az informatikai biztonság oktatásának elengedhetetlen feltétele az oktatás tárgyának és tartalmának pontos meghatározása. Ez viszont az informatikai biztonság rendszertanának leírását követeli meg. Kulcsszavak: információvédelem, információbiztonság, informatikai biztonság, informatikai rendszerek védelme, oktatás, rendszertan

Definition of the education's object and content is the essential condition of the information security education. However, this demand defines of the information security taxonomy. Keywords: information security, information systems security, education, taxonomy

Bevezetés

A Magyar Akkreditációs Bizottság (MAB) 2004 júliusában az akkreditációs útmutató 1. sz. mellékletében kötelező „főtantárgyként" írta elő a mérnök informatikusképzésben az informatikai biztonság alapjainak oktatását. Ezen túl is egyre többen és egyre többet próbálnak az informatikai biztonság kérdéseiben oktatni. Az oktatás szempontjából alapvető kérdés, hogy egy-egy tantárgy kereteiben mit oktassunk, a tantárgy mire terjedjen ki. Az informatikai biztonság oktatási területeinek meghatározását már korábban megpróbáltam [1]. Ennek során ismertem fel azt, hogy egy szakterület oktatását csak a szakterület rendszerezése alapján lehet meghatározni, először magának a szakterületnek a fogalmát, tartalmát és terjedelmét kell tisztázni, azaz az informatikai biztonságot, mint szakterületet, tudományszakot kell elemeznünk.

Egy tudományszak rendszerezése, tartalmi kérdéseinek pontos meghatározása fontos kérdés Sokan nem szeretnek, nem is akarnak ezzel

[1] A cikk a Robothadviselés 8. tudományos konferencián elhangzott Az információbiztonság egy lehetséges taxonómiája című előadás szerkesztett változata.

törődni, a „Költő vagyok — mit érdekelne engem a költészet maga…” [2] elvét vallják. Emellett az információbiztonság és az informatikai biztonság területén a különböző dokumentumok (jogszabályok, szabványok, ajánlások, kézikönyvek és más publikációk) eltérő szakkifejezéseket alkalmaznak, mutatva, hogy hazánkban még nem alakult ki egységes terminológia ezen a területen.

Természetesen már készültek különböző rendszertanok az információbiztonság és az informatikai biztonság területén, azonban ezek valamilyen más szempont alapján rendszerezik a kérdéskört. Ahhoz, hogy bármit is rendszerezzünk, meg kell határozni a rendszerezés alapját. Az alábbiak egy részét természetesen már felhasználták különböző rendszertanokban. A szakirodalomból ismert rendszertanok alapjaként a következőket használták fel:

— a védendő adat állapota az informatikai rendszerben (gyűjtés, tárolás, feldolgozás, továbbítás, törlés, stb.);
— a védendő tulajdonságok (bizalmassága, sértetlensége és rendelkezésre állás);
— a védelem feladatai (megelőzés, észlelés, reagálás, esemény- vagy válságkezelés);
— a védett rendszer gyenge pontjai (sebezhetőségei);
— a fenyegetések (az adat megsemmisülése, kompromittálódása, felfedése, tartalmának vagy tulajdonságának megváltozása, elérhetetlensége, megsemmisülése, ellen és helyreállítása);
— a fenyegetések okai (információs hadviselés, kiberterorrizmus, gazdaság hírszerzés, ipari kémkedés, számítógépes bűnözés, gazdasági bűnözés, képzetlenség, természeti csapások, műszaki hibák);
— a fenyegetések forrásai (pl. rosszindulatú programok);
— a fenyegetések célja (információszerzés, károkozás, stb.).

Alapmű az informatikai biztonság területén az úgynevezett Landwehr taxonómia [3], amely a fenyegetések származási forrását (ang.: Genesis) tekinti a rendszertan kiindulási alapjául. Vagy például Álláspont az információbiztosítás rendszertanáról munkájában Abe Usher [4] igen részletes áttekintést ad az informatikai biztonság részterületeiről, azonban nem a biztonság, hanem az információbiztosítás (ang.: information assurance) szempontjából kezeli a kérdést, illetve — véleményem szerint — túl sok felosztási szempontot (védelmi

intézkedések, biztonsági szolgáltatások és az információ állapota) alkalmaz.

Az informatikai biztonság rendszertanának meghatározásához az oktatási célú felhasználás elsődlegességéből kiindulva vizsgáltam meg a különböző rendszerezési lehetőségeket. A fogalmi kérdések meghatározásánál alapelvként kell kezelni, hogy „a terminológiai kérdések vizsgálata során a megnevezéssel szemben a tartalomnak van elsődlegessége" [5]. Ez az én értelmezésemben azt jelenti, hogy minden fogalom mögé precíz meghatározást kell állítani, és ez a meghatározás az elsődleges, és nem az a kifejezés, amihez tartozik.

Információbiztonság vagy informatikai biztonság

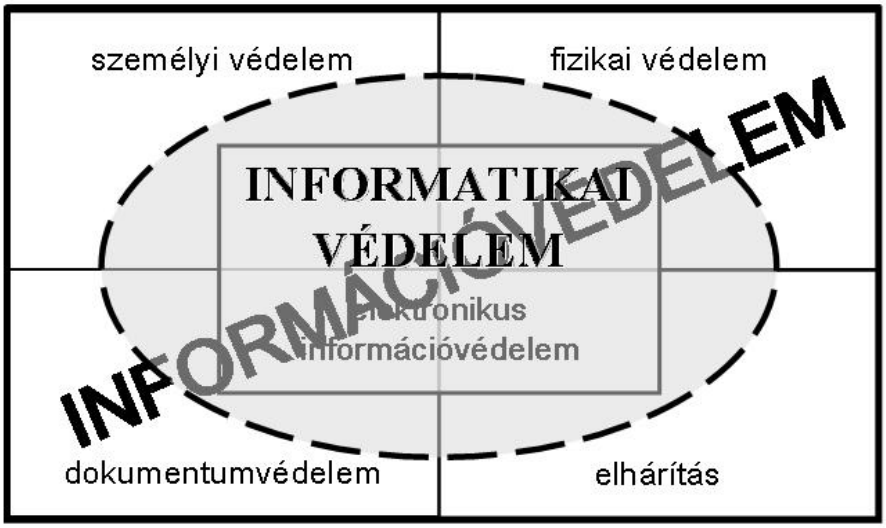
Az információbiztonságot és az informatikai biztonságot — néha még a szakemberek is — gyakran összekeverik egymással, sőt időnként az adatvédelemmel is. Az adatvédelem kifejezés — érdekes módon az angol nyelvben (data protection) is — a személyes adatok védelmére vonatkozik, a személyiségi jogokkal összefüggő tevékenység. Az információbiztonság és az informatikai biztonság különbözik egymástól. Az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ezzel szemben például az informatikai biztonság[2] „csak" az informatikai rendszerekben kezelt adatok, és az azt kezelő rendszer védelmét jelenti. Mivel angolul általában az információvédelemre, illetve az informatikai védelemre, sőt néha a kommunikációs, információs és más elektronikus rendszerek védelmére is az information security kifejezést használják, az egyes fordítások még inkább zavarossá teszik a képet. (A védelem és biztonság kifejezést egymás szinonimájaként használjuk, bár nem azonos a jelentésük. Erről a következő pontban még lesz szó.) Általában a szövegkörnyezet egyértelművé teszi, hogy információvédelemről vagy informatikai védelemről van szó. Például az ISO/IEC 27001:2005

[2] Az informatikai biztonság fogalmát magyarul először a MeH ITB 12. sz. ajánlás [6] készítése során határoztuk meg.

nemzetközi szabvány [7] eredeti angol címe az Information technology — Security techniques — Information security management systems — Requirements, aminek a kezdetén lévő Informa-tion Technology kifejezés — számomra — egyértelművé teszi, hogy itt az informatikáról van szó, majd ez után következik az Information security, ami így informatikai biztonságot jelent magyarul. Ezt a magyar szabványban [8] szó szerint információbiztonságnak fordították. (Sajnos a vonatkozó magyar szabványokban nem ez az egyetlen, és nem is a legnagyobb fordítási hiba.) A NATO védelmi előírása [9] szerint „Az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása, az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából". Az egyértelműség(?) kedvéért a NATO bevezette az INFOSEC kifejezést, amelyet az information security kifejezés szavainak összevonásával (INFOrmation SECurity) képeztek. Ezt a vonatkozó magyar szakirodalmakban általában elektronikus információvédelem vagy néha elektronikus dokumentumvédelem formában használják.

Az INFOSEC „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen". És ez meghatározás egyértelmű — az informatikai rendszerek, és az azokban kezelt adatok védelmére vonatkozik. Azonban ez az elektronikus információvédelem önmagában nem kezelhető, mert egy igen széles körű információvédelem része. Az informatikai védelem, pedig az információvédelemnél szűkebb, de "önállóan" is működtethető szakterület, amely a NATO INFOSEC-ben is meghatározott elektronikus információvédelmen kívül az információvédelem többi részét is magába foglalja, de csak az informatikai rendszer vonatkozásában. Más szóval az információbiztonság olyan területeit, mint a személyi védelem, a dokumentumvédelem, a fizikai védelem és az elhárítás (felderítés elleni tevékenység) az informatikai védelem esetében nem alkalmazzuk önállóan és teljes körűen, és csak az informatikai rendszer elemeinek

(fenyegetései elleni) védelmére. Az informatikai védelemnek ki kell terjedni az informatikai rendszer valamennyi elemére[3], de nem a teljes információs rendszerre. A következő ábrán az informatikai védelem és a NATO értelmezése szerinti információvédelem egymáshoz való viszonyát mutatom be.



Az informatikai rendszerek védelme

Az informatikai, a kommunikációs, és az egyéb elektronikus rendszerek között az egyes rendszerek kommunikációs vagy informatikai rendszerként való meghatározása egyre nehezebb (részletesen lásd még [10]). E technológiák konvergenciáját az informatikával és a távközléssel foglalkozó szakemberek már több mint egy évtizede vizsgálják.

Az információs társadalomhoz és a médiához kötődő iparágak konvergenciáról az Európai Unió az európai audiovizuális politika

[3] A rendszerelemek az informatikai rendszert és működési környezetét alkotó és működéséhez szükséges erők és eszközök (infrastruktúra, hardver, szoftver, dokumentáció és a rendszer kezelői, kiszolgálói és felhasználói, stb.). A pontos definíciót lásd később.

szabályozásának jövőjéről szóló közleménye megállapítja, hogy „Az információs társadalom fordulóponthoz érkezett: az elmúlt időszakban hatalmas technológiai fejlődés zajlott le, és az IKT[4] napjainkban lép a tömeges alkalmazás szakaszába … Műszaki szempontból a távközlési hálózatok, a médiumok, a tartalom, a szolgáltatások és az eszközök digitális konvergenciájával állunk szemben. … Az információs társadalom és a média területén működő szolgáltatások, hálózatok és eszközök digitális konvergenciája végre mindennapjaink valóságává válik …” [11].

Az információ- és kommunikációtechnológiák konvergenciája miatt magyarul az informatikai és kommunikációs technológia, néha az informatikai és kommunikációs rendszerek kifejezéseket használják, de az infokommunikációs technológia, vagy az infokommunikációs rendszerek kifejezést is alkalmazzák. A továbbiakban az egyszerűség miatt én az informatikai rendszer kifejezést fogom ebben a cikkben használni, és annak meghatározását a következőképpen fogadom el:

Informatikai rendszer az adatok kezelésére használt elektronikus eszközök, eljárások, valamint az ezeket kiszolgáló és a felhasználó személyek együttese.

Adatkezelés az adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatása, átalakítása, összegzése, elemzése stb.), továbbítása, törlése, hasznosítása (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása.

Ezek alapján az informatikai rendszerekhez tartoznak:

1. a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
2. a vezetékes, a mobil, a rádiós és műholdas távközlés;
3. a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
4. a rádiós vagy műholdas navigáció;
5. az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA[5], távmérő, távérzékelő és telemetriai rendszerek, stb.);
6. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

[4] IKT: információ- és kommunikációtechnológia, angolul: Information and Communication Technology (ICT)

[5] Supervisory Control and Data Acquisition (System) – vezérlő és adatgyűjtő rendszer

Ahhoz, hogy az informatikai rendszerek védelméről vagy biztonságáról tárgyaljunk, el kell fogadnunk magának a védelemnek és a biztonságnak a tartalmát. A védelem — a magyar nyelvben — tevékenység, illetve tevékenységek sorozata, amíg a biztonság egy állapot, amelyet a védelmi tevékenységgel lehet létrehozni. (A mindennapos szóhasználat a védelemre, a védelmi tevékenységre is a biztonság kifejezést használja!) A védelem feladatai:

1. megelőzés (ang.: prevention) és korai figyelmeztetés (ang.: early warning);
2. észlelés (ang.: detection);
3. reagálás (ang.: reaction);
4. esemény- (ang.: incident management) vagy válságkezelés (ang.: crisis management).

Általánosan elfogadott, hogy az informatikai rendszerek esetében a bizalmasság, sértetlenség és rendelkezésre állás megőrzése a cél. Az ISO/IEC 27001:2005 szabvány szerint „az informatikai védelmet az jellemezi, hogy megőrzi … a bizalmasságot …; a sértetlenséget …; a rendelkezésre állást …”[6] [7]. Ez ugyan egy szabványhoz képest kissé pongyola meghatározás, mert nem derül ki, hogy minek a bizalmasságát, sértetlenségét vagy rendelkezésre állását kell megőrizni, de vannak pontosabb meghatározások is.

Az előző pontban már említett NATO INFOSEC ennél sokkal precízebben meghatározza, hogy „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen” [9]. Ez szó szerint megegyezik Európai Unió Tanácsának Biztonsági Szabályzata [12] előírásaival.

Ezek alapján az informatikai rendszerek védelme a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre

[6] Angolul: *„Information security is characterized here as the preservation of: a) confidentiality …; b) integrity …; c) availability…”*

állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának megóvása. Ahol:

1. Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
2. Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség[7]) és a származás megtörténtének bizonyosságát (letagadhatatlanság[8]) is, illetve a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható.
3. Rendelkezésre állás: az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható.

A bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) hármasát szokták az angol kezdőbetűik alapján CIA-elvnek nevezni.

Az informatikai biztonság

A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Elfogadva, hogy a biztonság egy kedvező állapot, amellyel szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz azonban, hogy teljes legyen ez a biztonság az szükséges, hogy minden valós fenyegetésre valamilyen védelmet nyújtson, ugyanakkor körkörös legyen, vagyis minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy folyamatosan létezzen [6].

[7] ang.: authenticity
[8] ang.: non-repudiation

A fentiek alapján a biztonság a rendszer olyan — az érintett[9] számára kielégítő mértékű — állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ahol a zárt védelem az összes releváns fenyegetést figyelembe vevő védelmet, a teljes körű védelem, pedig a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. A folytonos védelem az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg. A kockázattal arányos védelem esetén egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel, azaz a védelemre akkora összeget és olymódon fordítanak, hogy ezzel a kockázat az érintett számára még elviselhető, vagy annál kisebb.

A biztonság fenti meghatározását elfogadva, levezethetjük az informatikai biztonság fogalmát. Ehhez kiindulópont, hogy a védelem alapvető tárgya az adat, de az adatot kezelő rendszerelemek is védendőek, hiszen ezek megfelelő állapota feltétele az adat védelmének. Mint már rögzítettük a fenyegetések az adatok bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetik, de nem közvetlenül érik az adatokat, hanem az azokat kezelő rendszerelemeken (pl. a hardver, szoftver, hálózat, személyek, …) keresztül érvényesülnek. Ennek figyelembe vételével, a biztonság általános definíciója alapján az infokommunikációs biztonságot a következőképpen határozom meg: Az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos [6], [13].

A fenyegetések elsősorban az adatok bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetik, de nem közvetlenül érik az adatokat, hanem az azokat kezelő rendszerelemeken keresztül érvényesülnek. A rendszer elemei a korábbi meghatározások [14], [6] szerint a következők:

[9] Az *érintett* alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő.

1. az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra;
2. hardver;
3. szoftver;
4. kommunikációs eszközök és hálózat;
5. adathordozók;
6. dokumentumok és dokumentáció;
7. személyek.

Az informatikai biztonság rendszerezésének alapja

Ahogy már a Bevezetésben írtam, a rendszerezéshez meg kell határozni a rendszerezés alapját. Az adat, a fenyegetések és a védelem — már mások által is feldolgozott — tulajdonságai nem szolgáltattak megfelelő alapot a rendszerezéshez. Ezért az informatikai biztonság definíciójában szereplő — még nem vizsgált — tulajdonságoknak a vizsgálatával folytattam. A biztonság tulajdonságai a következők

— zárt (az összes releváns fenyegetést figyelembe vevő védelem);
— teljes körű (a rendszer valamennyi elemére kiterjedő védelmi intézkedések összessége);
— folytonos (az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelem);
— kockázattal arányos (egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel, azaz a védelemre akkora összeget és olymódon fordítanak, hogy ezzel a kockázat az érintett számára még elviselhető, vagy annál kisebb).

Az oktatási célú felhasználás elsődlegességéből kiindulva megvizsgáltam a különböző rendszerezési lehetőségeket. Azt különösebb vizsgálat nélkül beláthatjuk, hogy a kockázattal arányosság és a folytonosság a rendszerezésre nem alkalmas tulajdonságok. A zártság, vagyis az összes releváns fenyegetést figyelembe vevő védelem már felhasználhatónak tűnt. Az Álláspont az információbiztosítás rendszertanáról tanulmányban [4] a rendszerezés egyik részszempontja a védelmi intézkedések (ang.: Secu-rity Countermeasures). Ezek részletes áttekintést adnak az informatikai biztonság egy részéről, de nem a egészéről. Azonban van egy nagy hibája. A védelmi intézkedések egyrészt az állandóan változó

fenyegetések miatt, másrészt a technológia fejlődése miatt folyamatosan változnak. Ez nem teszi alkalmassá, hogy egy rendszertan alapja legyen.

A teljes körűség a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. Ez alapján, a rendszerelemeken keresztül a rendszer biztonságához szükséges valamennyi védelmi intézkedés meghatározható.

A rendszerelemek alapján történő rendszerezés kellően részletezőnek, és stabilnak tűnik. Azonban a rendszerelemek korábban megadott felsorolása a rendszerezés szempontjából vizsgálva nem teljesen illeszkednek egy rendszertanba. A rendszerelemek tartalmi felsorolását megváltoztattam. Ebben a kockázatelemzés során a gyakorlatban[10] vizsgált területeket használtam fel.

Elsőként a személyek már régóta sérelmezett utolsó helyét cseréltem fel az elsővel. Ez csak egy sorrendi változtatás tűnik, de elvi jelentősége van.

A következő problémás elem az adathordozók. Nem teljesen használható a dokumentumoktól és dokumentációtól elválasztva, azaz az adatok és adathordozók egységes kezelése elvárás, tehát értelmetlen a külön rendszerelembe sorolásuk. Ugyanakkor megbízhatósági szempontból az adathordozók az adattárolás eszközei nélkül nehezen értelmezhetők. Ezért az adathordozókon belül az adattároló eszközöket, a dokumentumokat és dokumentációt is figyelembe kell venni.

A szabályozás korábban nem volt önálló rendszerelem, bár a kockázatelemzések során igen nagy szerepet kapott.

Az informatikai biztonság rendszertana

Az informatikai biztonság rendszertanának kiindulási pontjául tehát a védelem szempontjából figyelembe veendő rendszerelemeket fogadom el, és ezek a következők:

1. személyek;

[10] Közel 15 éve a gyakorlatban használom ezeket kockázatelemzéseknél. Ezek során voltak értelmezési gondjaink, amelyek a MeH ITB 8 sz. ajánlásának [14], mint kockázatelemzési módszertannak a használata során merültek fel. A rendszerelemek megnevezésének változtatása nélkül tartalmában már korábban is hasonlóan értelmeztük azokat.

2. az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra;
3. hardver;
4. szoftver;
5. kommunikációs eszközök és hálózat;
6. adathordozók;
7. szabályozás.

Az egyes rendszerelemekből kiindulva az alábbi rendszertan állítható fel:

1. Személyek (biztonsági elvárások és lehetőségek a megszerzés — megtartás — elbocsátás során):
   1.1. az alkalmazás előtt:
      1.1.1. a felvétel és a munkaköri leírások;
      1.1.2. a személyzet biztonsági átvilágítása és a személyzeti politika;
      1.1.3. a foglalkoztatás feltételei (felkészítés, jognyilatkozatok, munkavédelem, ember-gép kapcsolat, munkahelyi hardver- és szoftver-ergonómia);
   1.2. az alkalmazás alatt:
      1.2.1. a vezetőség felelősségei;
      1.2.2. az informatikai biztonsági oktatás és képzés (social engineering);
      1.2.3. felelősségre vonás, fegyelmi eljárás;
   1.3. az alkalmazás megszűnésekor vagy változásakor:
      1.3.1. a munkaviszony megszüntetésének vagy megváltoztatásának biztonsági kérdései;
      1.3.2. az átszervezés biztonsági kérdései;
      1.3.3. az eszközök visszaadása;
      1.3.4. a hozzáférési jogok visszavonása.
2. Az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra:
   2.1. „hagyományos” biztonság:
      2.1.1. beléptetés, élőerős őrzés;
      2.1.2. beléptető-rendszerek;
      2.1.3. elektronikai jelzőrendszer;
      2.1.4. videó rendszerek;
      2.1.5. mechanikai védelem (falak, rácsok, ajtók, ablakok);

2.1.6. tárolóeszközök (páncélszekrények, tűzálló-szekré-nyek, számítógéptermek);
2.2. tápáramellátás:
2.2.1. külső tápáramellátás;
2.2.2. szünetmentes tápegységek;
2.2.3. szükségáramforrások;
2.2.4. villám- és túlfeszültség-védelem;
2.2.5. a tápáramellátás zavarvédelme;
2.3. klimatizálás (hűtés – fűtés – páratartalom);
2.4. tűzvédelem:
2.4.1. passzív tűzvédelem;
2.4.2. tűzjelzés;
2.4.3. tűzoltóeszközök;
2.4.4. automatikus tűzoltórendszerek;
2.5. vízvédelem;
2.6. mechanikai rezgések elleni védelem;
2.7. helyiségek elektromágneses védelme:
2.7.1. elektromágneses kisugárzás elleni védelem;
2.7.2. szórt és vezetett elektromágneses zavarok elleni védelem;
2.7.3. elektromágneses kompatibilitás (EMC).
3. Hardver:
3.1. hibatűrő rendszerek és funkcionális redundancia:
3.1.1. redundanciamentes rendszerek;
3.1.2. redundáns struktúrák és redundáns struktúrákból felépülő összetett rendszerek (watchdog timer, watchdog processzor, master-checker, TMR, TANDEM non-stop architektúra, RAID);
3.1.3. megbízható szolgáltatások biztosítása:
3.1.3.1. a hibaáthidalás folyamatának kialakítása;
3.1.3.2. az újraindítási képesség megvalósítása;
3.2. eszközök elektromágneses védelme:
3.2.1. szórt és vezetett elektromágneses zavarok elleni védelem;
3.2.2. elektromágneses kompatibilitás (EMC);
3.2.3. elektromágneses kisugárzás elleni védelem (TEM-PEST).
4. Szoftver:
4.1. azonosítás és a hitelesítés:
4.1.1. az azonosítás és a hitelesítés folyamatának kialakítása;

4.1.2. hitelesítési szolgáltatások (Kerberos, Sesame, Radi-us és Diameter rendszerek, hitelesítő központok);
4.2. hozzáférés-jogosultsági és ellenőrzési rendszer:
4.2.1. a hozzáférés-jogosultság rendszerek, hozzáférés-vezérlési modellek (Mandatory Access Control, Discretionary Access Control, Rule Based Access Control, multilevel security), jogosultság kiosztás;
4.2.2. a hozzáférés-ellenőrzés rendszerének megvalósítása, jogosultság-ellenőrzés. A bizonyítékok rendszerének és folyamatának kialakítása
4.3. rosszindulatú programok elleni védelem:
4.3.1. vírusvédelem;
4.3.2. kémprogramok elleni védelem;
4.4. biztonságos programozás (programhibák, backdoor);
4.5. adatbázis biztonság.
5. Kommunikáció és hálózat
5.1. kriptográfia és biztonsági protokollok:
5.1.1. a rejtjelzés és az elektronikus aláírás kriptográfiai alapjai:
5.1.1.1. szimmetrikus blokk-típusú és folyam-típusú rejtjelzés (DES, IDEA, AES, GSM titkosítása);
5.1.1.2. aszimmetrikus rejtjelzés (RSA, DSA, elliptikus módszerek);
5.1.1.3. hash függvények.
5.1.1.4. szteganográfia, kvantum kriptográfia;
5.1.2. kriptográfiai protokollok:
5.1.2.1. kulcscsere protokollok;
5.1.2.2. tranzakció-biztonság (SSL);
5.1.3. kriptográfiai alkalmazások:
5.1.3.1. nyilvános kulcsú infrastruktúrák (PKI);
5.1.3.2. kulcstanúsítványok;
5.1.3.3. X.509 szabvány;
5.1.4. anonimizáló rendszerek (a személyes adatok védelme);
5.1.5. elektronikus fizetés, a SET protokoll;
5.1.6. mobil kereskedelem, mobil fizetési protokollok;
5.1.7. beszédtitkosító rendszerek;
5.1.8. a smart kártyák biztonsági (kriptográfiai) kérdései;
5.1.9. a virtuális magánhálózatok (VPN);

5.1.10. a vezeték nélküli hálózatok (WiFi) biztonsága;
5.2. hálózatszegmentálás:
5.2.1. routerek és switchek;
5.2.2. vezeték nélküli hozzáférési pontok;
5.2.3. demilitarizált zóna (DMZ);
5.3. határvédelem (perimeter defense):
5.3.1. hálózati címfordítás (NAT);
5.3.2. tűzfalak;
5.3.3. behatolás érzékelők és elhárítók;
5.3.4. rosszindulatú programok elleni védelem:
5.3.4.1. DoS, DDoS elleni védelem;
5.3.4.2. spamszűrés;
5.3.4.3. Java, Java applet-ek;
5.3.4.4. ActiveX;
5.3.4.5. cross site scripting;
5.3.5. a mézesmadzag (honeypot);
5.3.6. megbízható hálózatok:
5.3.6.1. hibatűrő hálózati architektúrák;
5.3.6.2. hozzárendelt és osztott védelem;
5.3.6.3. tükrözött és fürtözött szerverek.
6. Adathordozók:
6.1. adatkezelés:
6.1.1. nyilvántartás;
6.1.2. címkézés;
6.1.3. tárolás;
6.1.4. megsemmisítés;
6.2. adatredundancia;
6.3. kriptográfia és kódolás:
6.3.1. rejtjelzés;
6.3.2. digitális aláírás;
6.3.3. hibadetektáló és javító kódok;
6.3.4. tömörítő kódok;
6.4. biztonsági mentés-visszaállítás;
6.5. konzisztencia kezelés (dominó effektus);
6.6. redundáns struktúrák és redundáns struktúrákból felépülő rendszerek (RAID).

7. Szabályozás:
   7.1. kockázatelemzés, kockázatkezelés:
      7.1.1. audit;
      7.1.2. kockázatelemzés;
      7.1.3. értékelés és tanúsítás;
   7.2. az informatikai biztonság dokumentumai:
      7.2.1. informatikai biztonságpolitika;
      7.2.2. informatikai biztonsági szabályzat;
   7.3. szervezeti biztonság:
      7.3.1. az informatikai biztonság belső szervezeti struktúrája;
      7.3.2. előírások a külső személyek által történő hozzáférésekkel kapcsolatban;
      7.3.3. vállalkozásba adás;
   7.4. az eszközök biztonsági besorolása és ellenőrzése;
      7.4.1. számadási kötelezettségek az eszközökkel kapcsolatban;
      7.4.2. az adatok biztonsági osztályozása;
   7.5. személyi biztonság;
      7.5.1. az alkalmazás előtt;
      7.5.2. az alkalmazás alatt;
      7.5.3. az alkalmazás megszűnésekor vagy változásakor;

   7.6. fizikai és környezeti biztonság:
      7.6.1. biztonsági szegmensek;
      7.6.2. a berendezések fizikai védelme;
   7.7. számítógépes hálózati szolgáltatások és az üzemeltetés menedzsmentje:
      7.7.1. üzemeltetési eljárások és felelősségek;
      7.7.2. harmadik fél szolgáltatásának irányítása;
      7.7.3. informatikai rendszerek tervezése és átvétele;
      7.7.4. védelem rosszindulatú programok ellen;
      7.7.5. mentés;
      7.7.6. hálózatmenedzsment;
      7.7.7. az adathordozók biztonságos kezelése;
      7.7.8. adatok és programok cseréje;
      7.7.9. az elektronikus kereskedelem biztonsága;
      7.7.10. a biztonsági megfigyelő rendszer használata;
   7.8. hozzáférés menedzsment:

7.8.1. a hozzáférés ellenőrzés üzleti követelményei;
7.8.2. a felhasználói hozzáférés menedzsmentje;
7.8.3. a felhasználó feladatai, felelősségei;
7.8.4. a hálózati szintű hozzáférések menedzsmentje;
7.8.5. az operációs rendszerszintű hozzáférések ellenőrzése;
7.8.6. alkalmazás szintű hozzáférések vezérlése;
7.8.7. mobil informatikai tevékenység, távmunka;

7.9. fejlesztés és karbantartás:
7.9.1. az informatikai rendszerek informatikai biztonsági követelményei;
7.9.2. biztonság az alkalmazási rendszerekben;
7.9.3. kriptográfiai eszközök;
7.9.4. rendszerállományok védelme;
7.9.5. informatikai biztonság a fejlesztési és a karbantartási folyamatokban;
7.9.6. a műszaki sebezhetőségek kezelése;

7.10. biztonsági incidensek kezelése:
7.10.1. biztonsági események és biztonsági rések jelentése;
7.10.2. informatikai biztonsági incidenskezelés:
7.10.2.1. előkészületi módszerek és technológiák;
7.10.2.2. védelmi tervek;
7.10.2.3. az események észlelése, monitoring;
7.10.2.4. a kialakult események elemzése;
7.10.2.5. a bizonyítékok (adatok) gyűjtése, leltár;
7.10.2.6. kárenyhítés, helyreállítás;
7.10.2.7. nyomozás, felderítés;
7.10.2.8. jelentések és intézkedések;

7.11. működésfolytonosság:
7.11.1. katasztrófa-elhárítás tervezése;
7.11.2. üzletmenet-folytonosság tervezése;

7.12. jogszabályi (és társadalmi) megfelelőség:
7.12.1. adatvédelem: a személyes adatok védelme;
7.12.2. titokvédelem:
7.12.2.1. az államtitok és a szolgálati titok;
7.12.2.2. az üzleti titok, a banktitok, az értékpapírtitok és a biztosítási titok;
7.12.2.3. egészségügyi adatok;

7.12.3. elektronikus aláírás;
7.12.4. elektronikus szolgáltatások (e-kereskedelem);
7.12.5. az „internet-jog”;
7.12.6. szerzői jogok;
7.12.7. felhasználó-védelem (fogyasztóvédelem);
7.12.8. az etikus hackelés;
7.12.9. az informatikai rendszerek biztonsági ellenőrzésének szempontjai;

7.13. dokumentumkezelés, ügyvitel (iratkezelés).

Felhasznált irodalom

[1] Muha Lajos: Az informatikai biztonság oktatása, Felsőoktatási Matematika-, Fizika- és Számítástechnika Oktatók XXXI. Konferenciája, Dunaújváros, 2007.08.24. p.202-205.

[2] József Attila: Ars poetica

[3] LANDWEHR, C. E.: Formal models for computer security. ACM Computing Surveys 13, 3 (1981. szeptember), 247-278.

[4] Abe Usher: Towards a Taxonomy of Information Assurance, http://www.shap-ideas.net/ia/information_assurance.htm

[5] Munk Sándor: Információbiztonság vs. informatikai biztonság, Hadmérnök, különszám, http://www.hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf

[6] Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása. Budapest, 1996.

[7] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[8] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

[9] Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49

[10] Haig Zsolt: Az információbiztonság komplex értelmezése, Robothadviselés 6. tudományos szakmai konferencia, 2006. november 22.

[11] Az Európai Bizottság közleménye: i2010: európai információs társadalom a növekedésért és a foglalkoztatásért, Európai Közösségek Bizottsága, Brüsszel COM(2003) 784, 2005.01.06.

[12] Az Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK)

[13] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, doktori (Phd) értekezés – Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola, tudományos vezető: Dr. Kovács László mérnök őrnagy, 2007. – p10-20.

[14] Informatikai biztonsági módszertani kézikönyv, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 8. számú ajánlása – Budapest, 1994.